

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

PCT

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY
(PCT Rule 43bis.1)**

To:

see form PCT/ISA/220

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference
see form PCT/ISA/220

FOR FURTHER ACTION
See paragraph 2 below

International application No.
PCT/IB2017/050867

International filing date (day/month/year)
16.02.2017

Priority date (day/month/year)
23.02.2016

International Patent Classification (IPC) or both national classification and IPC
INV. H04L9/08 H04L9/30

Applicant
NCHAIN HOLDINGS LIMITED

1. This opinion contains indications relating to the following items:

- Box No. I Basis of the opinion
- Box No. II Priority
- Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- Box No. IV Lack of unity of invention
- Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement
- Box No. VI Certain documents cited
- Box No. VII Certain defects in the international application
- Box No. VIII Certain observations on the international application

2. FURTHER ACTION

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA:



European Patent Office
D-80298 Munich
Tel. +49 89 2399 - 0
Fax: +49 89 2399 - 4465


Date of completion of this opinion

see form PCT/ISA/210

Authorized Officer

Spranger, Stephanie

Telephone No. +49 89 2399-0



Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of:
 - the international application in the language in which it was filed.
 - a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1 (b)).
2. This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43bis.1(a))
3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing:
 - a. forming part of the international application as filed:
 - in the form of an Annex C/ST.25 text file.
 - on paper or in the form of an image file.
 - b. furnished together with the international application under PCT Rule 13ter.1(a) for the purposes of international search only in the form of an Annex C/ST.25 text file.
 - c. furnished subsequent to the international filing date for the purposes of international search only:
 - in the form of an Annex C/ST.25 text file (Rule 13ter.1(a)).
 - on paper or in the form of an image file (Rule 13ter.1(b) and Administrative Instructions, Section 713).
4. In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that forming part of the application as filed or does not go beyond the application as filed, as appropriate, were furnished.
5. Additional comments:

Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes: Claims	<u>2-26</u>
	No: Claims	<u>1, 27-29</u>
Inventive step (IS)	Yes: Claims	
	No: Claims	<u>1-29</u>
Industrial applicability (IA)	Yes: Claims	<u>1-29</u>
	No: Claims	

2. Citations and explanations

see separate sheet

Box No. VII Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

see separate sheet

Box No. VIII Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

see separate sheet

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1 Reference is made to the following documents:

- D1 WATANABE HIROKI ET AL: "Blockchain contract: A complete consensus using blockchain",
2015 IEEE 4TH GLOBAL CONFERENCE ON CONSUMER ELECTRONICS (GCCE), IEEE, 27 October 2015 (2015-10-27), pages 577-578, XP032858173,
DOI: 10.1109/GCCE.2015.7398721
[retrieved on 2016-02-03]
- D2 Andreas M. Antonopoulos: "Mastering Bitcoin - Unlocking Digital Cryptocurrencies"
In: "Mastering bitcoin : [unlocking digital cryptocurrencies]", 20 December 2014 (2014-12-20), O'Reilly Media, Beijing Cambridge Farnham Köln Sebastopol Tokyo, XP055306939,
ISBN: 978-1-4493-7404-4
- D3 KARL CRARY ET AL: "Peer-to-peer affine commitment using bitcoin",
ACM SIGPLAN NOTICES, ACM, 2 PENN PLAZA, SUITE 701 NEW YORK NY 10121-0701 USA,
vol. 50, no. 6, 3 June 2015 (2015-06-03), pages 479-488,
XP058070794,
ISSN: 0362-1340, DOI: 10.1145/2813885.2737997
- D4 AHMED KOSBA ET AL: "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts",
INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH,,
vol. 20150721:040253, 21 July 2015 (2015-07-21), pages 1-32,
XP061018923,
[retrieved on 2015-07-21]

2 The present application does not meet the criteria of Article 33(2) PCT, because the subject-matter of claims 1, 27, 28, and 29 is not new.

- 2.1 Document D1 discloses a method as claimed in claim 1 (reference to D1 is made in parenthesis):

A computer-implemented method for efficient transfer of a quantity of cryptocurrency on a peer-to-peer distributed ledger between a multiple of nodes, including a first transfer from a first node (*sender*) to a second node (*recipient*) (*fig.2,3*), the method comprising:

- receiving a first request (*transaction*) to transfer a first quantity of cryptocurrency associated with the first transfer from the first node to the second node (*fig.2*);
- determining a second node master public key associated with the second node, wherein the second node master public key forms a cryptographic pair with a second node master private key (*fi.3, sec. 1: bitcoin: implicit to bitcoin see e.g. D2 chap. 4, "hierarchical deterministic wallets"*);
- determining a generator value (*fig.3, sec. 1: bitcoin: implicit to bitcoin see e.g. D2 chap. 4, "hierarchical deterministic wallets"*);
- determining a second node second public key based on at least the second node master public key and the generator value (*fig.3, sec. 1: bitcoin: implicit to bitcoin see e.g. D2 chap. 4, "hierarchical deterministic wallets"*);
- determining a first output script (*fig.2, 3*), wherein the first output script is based on:
 - at least a first metadata that includes information associated with the first transfer (*contract information*); and
 - the second node second public key (*address of destination, also implicit to bitcoin see e.g. D2 chap. 4, "hierarchical deterministic wallets"*);
- sending, over a communications network, a first data output to a peer-to-peer distributed ledger (*blockchain*) based on:
 - an indication of the first transfer from the first node to the second node (*fig.2*);
 - and
 - the first output script, wherein the first output script is associated with the first quantity of cryptocurrency (*fig.2*).

- 2.2 The same reasoning applies, mutatis mutandis, to the subject-matter of the corresponding independent claims 27, 28, and 29, which therefore are also considered not new.

- 3 Dependent claims 2-26 do not contain any features which, in combination with the features of any claim to which they refer, meet the requirements of the PCT in respect of novelty and/or inventive step since their features (payroll, key pairs, hierarchical wallet, specification of second public key in the

transaction metadata, specification of generator value, shared secret agreed on) are either known from the prior art (documents D1-D4; see in particular passages cited in the search report) or merely represent minor implementation details to the person skilled in the art.

Re Item VII

Certain defects in the international application

- 4 The features of the claims are not provided with reference signs placed in parentheses to increase the intelligibility of the claims (Rule 6.2(b) PCT).
- 5 The most relevant prior art documents D1-D4 are not identified in the description and the description is not adapted to the independent claims (Rule 5.1(a)(ii)(iii) PCT).

Re Item VIII

Certain observations on the international application

- 6 The application does not meet the requirements of Article 6 PCT, because claims 21 and 22 are not clear. In particular, from the wording of the claims it is not clear whether the claims are dependent from claim 20 although the claims appear to comprise all features from claim 20.